Policies and standards: which few do you need, and does anyone follow them?

This quarter, cut your security documents to one management-approved information security policy, an acceptable use page and about six topic policies of short, testable "must" rules, each with an owner and, wherever possible, a setting that enforces it. Review them at least yearly and after significant incidents or changes by checking each rule against the live settings, and keep one mapping table so the same set serves ISO 27001, Grundschutz++ and NIS2 audits.

Reviewed	Next review	Version
5 Nov 2026	**5 Dec 2026**	**1.0**

Written for

Heads of security, CISOs and IT leads who write security policies, and the managing directors who approve them, especially under NIS2 or the BSIG

Latest version

sheets.einblick.dev/policies-standards/

If you only do five things

1. **Keep one short, signed policy on top.**
   Two to five pages: scope, objectives, roles, topic policies, approval date. The BSI says more than 20 pages hasn't worked in practice[9].
2. **Cut the rest to about six topic policies.**
   ENISA counts ten that 2024/2690 requires of digital providers and lets you merge them[3].
3. **Write rules you can test.**
   One sentence per rule, saying who must do what, and one owner per document. Mark advice as advice, as the NCSC asks[15].
4. **Put a setting behind each rule.**
   Enforce it in Intune, Group Policy or Conditional Access (Entra ID P1)[17]. The CAF rates total reliance on users' manual care as not achieved[16].
5. **Review against the settings, not the calendar.**
   Each year, compare every rule with a settings export, open exceptions and recent incidents, and log what changed.

Four document levels, and who signs each

1. **Policy: what and why?**
   Intentions and direction formally expressed by management, as ISO/IEC 27002 defines a topic-specific policy[3]. 2024/2690 has digital providers' management body approve the top policy, an appropriate level of management the topic policies[2].
2. **Standard: which settings, exactly?**
   Mandatory settings, such as MFA methods, patch deadlines and baselines; NIST calls standards normally compulsory[14]. Our rule: the heads of security and IT approve them.
3. **Procedure: which steps?**
   Steps for one task, such as creating an admin account[14]. The process owner approves them; in BSI terms, Arbeitsanweisungen[9].
4. **Guideline: what do we advise?**
   Advice that can be followed in more than one way[14], published by its author without formal approval.

The documents you actually need

- **Information security policy.** Approach, objectives, resources, roles, topic policies, records, indicators and approval date, from 2024/2690's list[2]. ENISA maps it to ISO 27001 clause 5.2 and A.5.1[4].
- **Acceptable use.** One or two pages on devices, accounts, data, AI tools, reporting and sanctions[8]. Training: the security awareness sheet.
- **Risk management.** Method and acceptance[1]; see the risk register sheet.
- **Access control.** Accounts, MFA, admin accounts, joiners and leavers[2].
- **Incidents, continuity and backup**[1]; see the incident response, backups and business continuity sheets.
- **Suppliers.** Criteria and contract clauses[2]; see the third-party risk sheet.
- **Data handling and encryption.** Classification, media, disposal, keys[2].
- **Development, change and testing,** if you build or run software.

Write rules people follow

- **One rule, one sentence, one "must".** "Admins must sign in with a security key" can be tested; "appropriate authentication" can't. Write advice as "should", so staff can tell the two apart[15].
- **Name the owner, setting and evidence.** The owner keeps the document current[9]; each rule names its setting and the report that proves it.
- **Write for the reader.** One page for staff, standards for admins. The CAF rates rules too detailed to remember as not achieved[16].
- **Ask the people who do the work** whether each rule is usable[15].
- **In Germany, involve the works council.** It co-determines rules on staff conduct and technical monitoring (BetrVG § 87(1) nos. 1 and 6)[24].

What changed in 2026

- **German duties apply.** Since 6 December 2025, with no general transition period, the BSI expects processes, responsibilities and measures in writing and reviewed regularly[6].
- **Grundschutz++ arrived.** BSI-Standard 300-1 (20 October 2026) has management release the policy and requires document control[10]. Certification applications open on 1 January 2027; classic IT-Grundschutz stays certifiable until 30 November 2031[11].

Approval and review

- **NIS2.** Management bodies approve the measures, oversee them and can be held liable[1]; digital providers date the approval in the policy[2].

Versions, publishing and sign-off

- **Same header everywhere.** Title, owner, version, last and next review, approval, classification and distribution[9], plus a change log.

- **Germany.** BSIG § 38 has management implement and oversee the § 30 measures, whose compliance must be documented[5]. Minute the approval; the BSI recommends resolutions as proof of involvement[7].
- **Topic policies one level down,** by the role the top policy names.
- **Yearly and on triggers.** Digital providers' management reviews the top policy at least annually and after significant incidents or changes[2]. Add new laws, audit findings[3], new technology or an acquisition[13].
- **Stagger the rest:** review each yearly[9], two or three a quarter.

Exceptions

- **Write the route into the top policy.** ENISA expects one, with requests, approvals and compensating controls on record and open exceptions reported to management. It has management bodies approve exceptions to the top policy itself[3]. Other levels: the risk register sheet.
- **Count them per rule at each review.** A rule that collects exceptions needs rewriting or funding.

Mistakes that cost the most

- **A template nobody adapted.** It names tools you don't run. Yet SANS's templates, made with CRF[20], can't be adapted without permission: SANS allows personal, non-commercial use without changes[21], CRF internal business use without derivative works[22]. Use them as checklists.
- **Settings that contradict the policy.** It demands 90-day password changes, NIST says not to[23], and your tenant doesn't.
- **Reviews that only change the date.** A new date without a change log shows nobody weighed the incidents and findings.
- **A signed policy as the goal.** The BSI asks for proof of effectiveness[7].

- **One source, one place to read.** A versioned library or Git, one intranet page and old versions archived centrally[8].
- **Acknowledge at hire, yearly and on change**[13]. 2024/2690 requires it for the top policy, from relevant staff and external parties[2]; ENISA accepts a digital one or a contract clause[3].
- **Collect it at sign-in.** Entra terms of use (Entra ID P1) can require reacceptance of each version; deleting the terms or losing P1 deletes the records, so export them[18].

One set for several audits

- **One table, one row per rule:** owner, setting, evidence, ISO 27001 Annex A control, Grundschutz++ or IT-Grundschutz requirement, NIS2 Article 21(2) point, BSIG § 30(2) number.
- **Start from official tables.** ENISA maps 2024/2690 to ISO/IEC 27001:2022 and CSF 2.0[4], the BSI § 30 BSIG to ISO 27001[12]. A mapping isn't equivalence, ENISA warns[3]. Certification: the ISMS sheet.

What you can skip

- **A 40-document library.** ENISA accepts the topic policies in one document[3].
- **Signatures on every standard.** Staff acknowledge the top policy and the acceptable use page.
- **A policy tool before the first review.** A versioned library and one intranet page will do.
- **One set per framework or customer.** Add a mapping column instead.
- **Legal prose.** Short sentences hold up better in audits.

What this looks like at your size

Small team, no security staff

- Write the top policy and acceptable use page with your IT provider; the managing director signs.
- Adapt CIS's acceptable use template for internal use; don't publish or sell your version[19].
- Collect acknowledgment at onboarding and yearly.

Growing, with IT or security staff

- Keep a top policy, acceptable use and six topic policies with owners, and standards below them.
- Collect acknowledgment with Entra terms of use.
- Review two or three documents a quarter against settings exports.

Enterprise or regulated

- Approve one group policy and have each regulated entity's management adopt it with local annexes.
- Keep the mapping table in the GRC tool, linked to configuration checks.
- Have internal audit test a sample of rules yearly.

Version history

5 Nov 2026, version 1.0	Published after a copy edit and a source-by-source fact check, which told companies what SANS, CRF and CIS template terms allow, added the risk management policy, labeled 2024/2690 duties as applying to digital providers and noted that Entra terms of use records vanish when deleted or unlicensed.

Sources

1. NIS2 Directive, Articles 20 and 21. EUR-Lex, 2022. eur-lex.europa.eu
2. Regulation (EU) 2024/2690. EUR-Lex, 17 Oct 2024. eur-lex.europa.eu
3. NIS2 Implementation Guidance, v1.0. ENISA, 26 Jun 2025. enisa.europa.eu
4. NIS2 guidance mapping table, v1.2. ENISA, 21 Aug 2025. enisa.europa.eu
5. BSIG §§ 30 and 38. BMJV, checked 5 Nov 2026. gesetze-im-internet.de
6. Fragen und Antworten zu NIS-2. BSI, checked 5 Nov 2026. bsi.bund.de
7. Curriculum Geschäftsleitungsschulung. BSI, 28 Oct 2026. bsi.bund.de
8. ISMS.1 Sicherheitsmanagement, Edition 2023. BSI, 2023. bsi.bund.de
9. BSI-Standard 200-2, chapters 3.4 and 5.2. BSI, Oct 2017. bsi.bund.de
10. BSI-Standard 300-1, v1.0. BSI, 20 Oct 2026. bsi.bund.de
11. Grundschutz++ milestone plan. BSI, Oct 2026. bsi.bund.de
12. #nis2know: ISO/IEC 27001. BSI, checked 5 Nov 2026. bsi.bund.de
13. CSF 2.0 Implementation Examples, GV.PO. NIST, 26 Feb 2024. nist.gov
14. SP 800-12 Rev. 1, chapter 5. NIST, Jun 2017. csrc.nist.gov
15. Cyber security culture principle 6. NCSC (UK), 4 Jun 2025. ncsc.gov.uk
16. CAF 4.0, principle B1. NCSC (UK), 2025. ncsc.gov.uk
17. Conditional Access overview. Microsoft Learn, 27 Apr 2026. learn.microsoft.com
18. Microsoft Entra terms of use. Microsoft Learn, 24 Mar 2026. learn.microsoft.com
19. CIS v8.1 Acceptable Use Policy Template. CIS, 29 Oct 2025. cisecurity.org
20. Cybersecurity policy templates. SANS Institute, 11 Feb 2026. sans.org
21. Terms and Conditions. SANS Institute, checked 5 Nov 2026. sans.org
22. Terms of Use. Cybersecurity Risk Foundation, 1 Mar 2025. crfsecure.org
23. SP 800-63B-4. NIST, Jul 2025. nvlpubs.nist.gov
24. BetrVG § 87. BMJV, checked 5 Nov 2026. gesetze-im-internet.de